THE ENABLING OPERATIONS IN CYBERSPACE THROUGH INSTITUTIONAL AND OPERATIONAL UNITY OF EFFORT WHITE PAPER

9 JULY 2013

Headquarters, United States Army Training and Doctrine Command
Army Capabilities Integration Center
Concepts Development and Learning Directorate
Fort Eustis, VA 23604

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
09 JUL 2013	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Enabling Operations in Cyberspace Through Institutional and Operational Unity of Effort White Paper	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Joint and Army Concepts Division - Concept Development and Learning Directorate - U.S. Army Capabilites Integration Center	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army Capabilities Integration Center 950 Jefferson Avenue Fort Eustis, Virginia 23604	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Enabling Operations in Cyberspace through Institutional and Operational Unity of Effort white paper establishes the baseline for follow-on analysis by the TRADOC-sponsored Cyberspace Working Group of the Mission Command Integrated Capability Development Team (ICDT). It develops the logic for establishing unity of effort in developing and employing cyberspace capabilities to enable mission command. The white paper presents a conceptual description of how Army commanders integrate cyberspace operations through organic capabilities, across all domains and with all warfighting functions (WfF) to conduct unified land operations and retain freedom of action while denying the same to adversaries in the 2013-2017 timeframe. This paper does not explore the role of cyberspace in relation to inform and influence activities.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**38**	

This pamphlet is available on the ARCIC Portal at https://cac.arcicportal.army.mil/sites/cde/condev/White%20Papers%20and%20CONOPS/Forms/AllItems.aspx

Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Eustis, Virginia 23604

9 July 2013

Military Operations

ENABLING OPERATIONS IN CYBERSPACE THROUGH INSTITUTIONAL AND OPERATIONAL UNITY OF EFFORT WHITE PAPER

History. This white paper is a new publication.

Summary. This white paper describes the requirement for the Army to develop unity of effort during the development and employment of cyberspace capabilities to enable missions command.

Applicability. This white paper applies to all U.S. Training and Doctrine command (TRADOC), Department of Army (DA), U.S. Army Reserve and U.S. Army National Guard component activities that develop Army cyberspace doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) requirements and capabilities.

Proponent and supplementation authority. The proponent of this paper is the TRADOC Headquarters, Director, Army Capabilities Integration Center (ARCIC). The proponent has the authority to approve exceptions or waivers to this paper that are consistent with controlling law and regulations. Do not supplement this paper without prior approval from Director, TRADOC ARCIC (ATFC-ED), 950 Jefferson Avenue, Fort Eustis, VA 23604-5763.

Suggested improvements. Users are invited to submit comments and suggested improvements via The Army Suggestion Program online at https://armysuggestions.army.mil (Army Knowledge Online account required) or via DA Form 2028 to Director, TRADOC ARCIC (ATFC-ED), 950 Jefferson Avenue, Fort Eustis, VA 23604. Suggested improvements may also be submitted using DA Form 1045.

Availability. This pamphlet is available on the ARCIC Portal at https://cac.arcicportal.army.mil/sites/cde/condev/White%20Papers%20and%20CONOPS/Forms/AllItems.aspx

Contents **Page**

Chapter 1
Introduction

1-1. Purpose
The "Enabling Operations in Cyberspace through Institutional and Operational Unity of Effort" white paper establishes the baseline for follow-on analysis by the TRADOC-sponsored Cyberspace Working Group of the Mission Command Integrated Capability Development Team (ICDT). It develops the logic for establishing unity of effort in developing and employing cyberspace capabilities to enable mission command. The white paper presents a conceptual description of how Army commanders integrate cyberspace operations through organic capabilities, across all domains and with all warfighting functions (WfF) to conduct unified land operations and retain freedom of action while denying the same to adversaries in the 2013-2017 timeframe. This paper does not explore the role of cyberspace in relation to inform and influence activities.

1-2. Background
The Chief of Staff, U.S. Army (CSA) conducted a series of senior leader summits in 2012 to identify the DOTLMPF gaps for Army operations in and through the cyberspace domain. These sessions showed that the Army lacked a clear vision of the roles the Army staff, TRADOC, U.S. Army Cyber Command (ARCYBER), force modernization proponents, capability developers, and materiel developers have in enabling operations in and through cyberspace. Therefore, the CSA directed TRADOC to analyze how the Army enables operations in and through the cyberspace domain. The commanding general, TRADOC directed the development of this white paper, and the establishment of a working group to identify a holistic concept and capability development strategy.

1-3. References
Required references and related publications are listed in appendix A. This reference section provides the results of a literature review through the use of an annotated reference section.

1-4. Explanation of abbreviations and terms
Abbreviations and special terms used in this pamphlet are explained in the glossary. To help clarify the lexicon, the glossary includes commonly used terms in the terms and special terms portions of the glossary.

Chapter 2
Operational Context

2-1. The information environment

a. The information environment is a critical factor in any operation, as it has the greatest impact on humans, and has a lasting effect in changing human societies.[1] The information environment exists in all physical domains–land, air, maritime, and space. It encompasses the physical, informational, and cognitive actions for collecting, processing, disseminating, and acting upon information. In military operations, most information is received via auditory or

visual signals. The majority of these signals are transmitted via the electromagnetic spectrum (EMS) by information systems.[2,3]

b. Three categories of information systems affect both Army and adversary operations: commercial; non-commercial (either academic or non-Department of Defense (DOD) governmental); and military.[4] Within these categories, Army forces are most affected by media and cyberspace.

(1) Media include social media interfaces, (such as Twitter®, Facebook®), web-based blogs, public media (such as, television, radio), and the physical dimension of the information environment commonly associated with printed periodicals. Media is focused on information content.

(2) Cyberspace exists in the information environment and consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[5] It is created, owned, maintained, and operated by public, private, and government stakeholders globally. Traditionally based on wired networks, the Internet has morphed to a wireless enterprise that includes applications and processes used to access, store, display, and manipulate information.[6] These wireless networks normally include a wired network which transitions the signal to longer range transmission system whether in the land or space domains.

(a) Today, most telecommunications use (in whole or in part) the EMS to transmit either analog or digital information. The EMS includes wired, wireless voice communications, text messaging, video conferencing, and radio frequency transmissions. Wireless technologies currently include cellular, space based, point-to-point, and line-of-sight systems. Telecommunications focuses on information transmission.

(b) Though cyberspace exists in the information environment, the infrastructure which makes cyberspace possible exists in the physical domains. This unique characteristic of cyberspace presents both challenges and opportunities for the U.S. Army.

c. Three dimensions the information environment.

(1) The information environment has three dimensions, equally important during military operations, so the boundaries between many aspects of the information environment become less distinct.[7] As this trend occurs, the speed of interaction between humans and the information upon which they act increases dynamically. Recognizing this increase in the velocity of information transfer, combined with technological convergence and increase in capability, the way in which the information environment is leveraged during operations is changing rapidly.

(2) Divisions between media and cyberspace mean little when Internet-based social media becomes the input for traditional public media. Low-cost, cellular-based smart phones serve as telecommunication devices and computers without the need for an extensive wired infrastructure. Internet-based programs, such as Skype®, provide video conferencing, text, and social media capabilities on mobile devices and on established commercial, non-commercial, and DOD

networks. These technology-focused interactions allow users in underdeveloped regions of the world to use a single device as a computer processor for social media service and a telecommunications network device to upload a photo onto a mass media Internet site without the additional cost of a wired infrastructure to link each user.

(3) The use of social media to disseminate messages and create social action (such as, initiate a flash mob) instantly, regardless of the system used to disseminate the message, challenges military operations by reducing reaction times, as was recently observed in Tunisia. This convergence within the information environment has driven the DOD to reexamine the relationship between EMS and cyberspace, and their combined use in telecommunications and media.

d. The joint information environment (JIE) is the DOD response to the dynamic information environment.[8] The JIE recognizes that U.S. operations require a holistic approach to provisioning technologies, and to developing information technology, services, and security architectures that allow commanders to receive the right information at the right time and in the right format.[9] The Army's most significant contribution to the JIE is LandWarNet.[10]

e. The role of the information environment during operations has not changed. What has changed is the medium in which the Army creates, modifies, stores, and exchanges information to engage with unified action partners and dominate adversaries. The speed at which a commander receives and responds to the transfer of information has also changed. However, most adversaries will conduct operations in the information environment without the legal and moral constraints of U.S. forces. Army leaders must be able to overcome this challenge to achieve enduring results.

2-2. Drivers of change

a. The emerging operating environment combines heavily networked friendly forces operating against a heavily networked adversary amongst a heavily networked society. Several key drivers of change influence this evolving environment.

b. Proliferation of cyberspace capabilities. At least 120 countries have, or are developing, cyberspace espionage and cyberspace war capabilities.[11] Attacks from cyberspace against U.S. financial, government, public and private infrastructure, private sectors, and institutions occur daily. Competitors, potential adversaries, and individual actors have linked achievement of their strategic goals to outcomes in the information environment. Competitors such as Russia and the People's Republic of China, and adversaries such as Iran and the Democratic People's Republic of Korea, terrorist, criminal, and "hacktivist" organizations have sought technological capabilities to conduct attributable and non-attributable operations in the information environment.[12]

c. Military applications. The Army depends on cyberspace to function and gain an information advantage over adversaries of the U.S. Commanders and leaders at all echelons use cyberspace to enable military, intelligence, and business operations, including the movement of personnel and materiel and the conduct of mission command through the full range of military

operations (ROMO). The July 2011 DOD Strategy for Operating in Cyberspace's direction to treat cyberspace as an operational domain to take full advantage of cyberspace's potential reflects DOD and Army reliance on cyberspace.[13] The Army's reliance on cyberspace as an operational domain cannot be overstated.

d. Ethical dilemmas. The U.S. Army will face an adversary, whose operations in cyberspace are less encumbered by treaty, law, and policy restrictions than those imposed on U.S. forces, allowing an adversary to seize and retain freedom of action. These dynamics are exacerbated as nation-state and individual actors operate together for strategic goals. Nation-states will continue to enable individual actors through access to infrastructure and expertise while the individual actors provide non-attributable actions in support of the nation-states' strategic goals.

e. Easy access. Ubiquitous, low cost mobile devices, sensors, and smart systems communicating independently without the need for additional infrastructure investment allow a greater number of more technology-savvy actors to operate in the cyberspace domain. Thus, state and non-state actors are concerned with the increased dependence on cyberspace, and the means to exploit, control, leverage, and manipulate the domain. This concern will lead to the extensive use of cyberspace capabilities as an integral aspect of political and military competition, and the potential for cyberspace innovation to originate outside the U.S.

f. Fast power.[14] Fast power is the ability to shape events at speed effectively; access in and through cyberspace is the linchpin of this power. Fast power forces governments and militaries to react at speed to events as they unfold. For the military, operations in cyberspace enable the application of fast power by unified action partners and adversaries in non-traditional ways across the ROMO. Commanders must be cognizant of applying fast power incorrectly, which results in lost opportunities.

g. Lessons from the 2008 Russian-Georgian conflict, Operation Enduring Freedom, and Operation Iraqi Freedom drive the need to evaluate how the U.S. Army integrates the cyberspace domain with the physical domains. Commanders require the ability to address cyberspace as a multi-domain operation. Commanders must integrate their capabilities (tasks and systems) across all domains to seize, retain, and exploit an advantage over adversaries and protect the mission command system (MCS), while simultaneously denying the same to adversaries.

2-3. The growing interdependence of the land, cyberspace, and human domain[15]

a. The Army operates in the principal domains in which humans interact. This includes a physical presence in the land domain and a virtual presence in the cyberspace domain. The human domain connects all domains, and establishes the purpose for conducting integrated operations in the physical and cyberspace domains. U.S. Army presence in the physical and virtual domains provides opportunities to understand the environment rapidly, set conditions for operations, and create enduring change in the human domain by affecting the behaviors of individuals, leaders, and nations. The interaction between domains presents risk if the Army does not operate effectively in all domains. The Army must achieve cross-domain synergy across the ROMO and all phases of a joint operation, and cannot concede advantages in any domain (see figure 2-1).

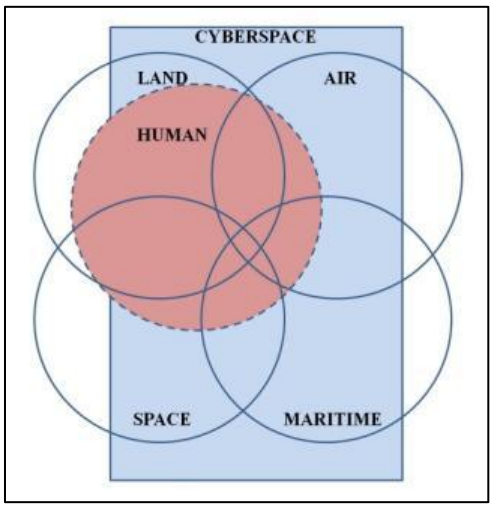

Figure 2-1. Domain interaction

b. For years, the Army has leveraged cyberspace to enable rapid and highly dispersed operations by tightly integrated teams.[16] Cyberspace capabilities increase the effectiveness of Army forces through strategic flexibility and global responsiveness. Emerging concepts for operating in cyberspace envision virtual personas and partnerships complementing the Army's physical presence.[17] For example, virtual presence allows a commander and unit to conduct a variety of activities by replicating their physical presence in an area of responsibility (AOR) or to have an effect at a place other than their actual location. This is not unlike the long-range unmanned aerial systems whose pilot may be thousands of miles away from the AOR. The emergence of virtual partnerships, conducted remotely with allies and friendly nations, can help build relationships that promote specified U.S. interests, build allied and friendly nation capabilities for self-defense and coalition operations, and provide U.S. forces with peacetime and contingency access.

c. As the nation's primary providers of landpower, the Army and Marine Corps are unique in their ability to employ a full array of capabilities while simultaneously controlling the application of violence. Army commanders scale the application and use of violence from deterring potential adversaries through the mere threat of the use of force, through the application of nonlethal capabilities, to the application of lethal elements of combat power to defeat enemies. Fully developing cyberspace capabilities provides the combined arms team with trained and readily available capabilities to deter and defeat adversaries across all domains.

Chapter 3
Enabling the Army in Cyberspace

3-1. Shifting the Army's focus

a. The Army employs its cyberspace capabilities to support the strategic missions of U.S. Cyber Command (USCYBERCOM); build, operate, maintain, and defend Army networks; and enable defensive and offensive operations at the operational and tactical echelons.

b. Commanders gain advantages over adversaries in the physical domains by seizing the initiative in cyberspace. Freedom of action in cyberspace allows access to joint enablers at lower echelons, provides for distributed operations, and speeds a commander's decision cycle while denying the same to the adversary. Operations in cyberspace focus on gaining these advantages and preventing the adversary from using cyberspace to enable their operations. Commanders must have the ability to conduct combined arms maneuver and wide area security in both cyberspace and the physical domains.

c. The development and application of cyberspace capabilities is dispersed across the Army. Currently there are over five organizations directly involved in defining the requirements to operate in cyberspace, which means that TRADOC, ARCYBER, and the DA headquarters staff routinely present the materiel developers with competing requirements.

d. The operational environment (OE) requires Army commanders to operate effectively in the cyberspace domain with the authorities provisioned in titles 10, 32, and 50 of the United States Code (USC). As more space, cyberspace, and EMS commercial-off-the-shelf technologies are pushed to the tactical edge, commanders are confronted with the complexities of supporting information technology procurement and management mandates discussed in Title 40 USC, the implementation of information security control requirements outlined in Title 44 USC; and the use of commercial technology infrastructure in accordance with Title 47 USC.

e. Currently, commanders do not have the ability to think globally and act locally through local offensive cyberspace operations. Army forces lack the software, hardware, and people with the necessary expertise to create local effects.[18] Because Army commanders cannot confine the effects of offensive cyberspace operations to their assigned areas of operation (AO), policy requires extensive coordination and review prior to execution of a cyberspace operation. Instead, commanders choose to rely on electronic and physical means to deter or defeat adversary capabilities.

3-2. Problem

How should the Army organize to develop the concepts and capabilities required to man, equip, and train institutional and operational forces and conduct integrated cyberspace operations to enable freedom of action at strategic, operational, and tactical echelons as part of unified land operations?

3-3. Solution: Institutional and operational unity of effort

a. Institutional unity of effort.

(1) Unity of effort in the development of concepts and capabilities to conduct cyberspace operations is critical. Without it, operational commanders and Soldiers will carry the burden of integrating disparate cyberspace operations capabilities. Unity of effort begins with a clearly defined force development proponent that integrates policy with concepts and capability developments and manages the seamless transition between the institutional force (capability

developers, materiel developers, leader development and training developers), and the operating force.[19]

(2) The Army has designated several force modernization proponents to develop the capabilities needed to achieve cyberspace operations. This approach has reduced the ability of the Army to provide an integrated solution strategy, focused on achieving true unity of effort within the institutional force and across the institutional and operating forces. In the past, the Army addressed this type of integration challenge by consolidating force modernization proponents, co-locating multiple proponents, or aligning the chain of command of capability developers, and ensuring the roles of policy and capability developers where not intermingled. An example of creating integration is the sustainment community's development of the multifunctional logistics organizations. Another useful model is the early 2000's model of the Combined Arms Center as the senior headquarters for all combat and combat support force modernization proponents.

b. Operational unity of effort. When conducting operations, commanders think and operate across the human domain, physical domains, the cyberspace domain, and the EMS to gain and maintain public support for the mission; decisively win the technological competition in space, cyberspace, and the EMS; and dominate in a contest of wills against determined enemies and adversaries. Commanders integrate activities within the information environment with activities in the physical domains to affect change in one or more domain and achieve cross-domain synergy.[20] Commanders utilize the MCS to conduct cyber electromagnetic activities to generate effects utilizing Title 10 USC capabilities under inherent Title 10 USC authorities.

Chapter 4
Enabling Operations In and Through Cyberspace

4-1. Defining cyberspace operations

a. Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[21] Cyberspace operations include the tasks and activities that enable freedom of action within cyberspace and the EMS and deny the same to adversaries.

b. Activities that utilize cyberspace capabilities to achieve non-cyberspace effects should not be categorized strictly as cyberspace operations. For example, creating a leaflet in support of military information support operations and sending it to a networked printer is not a cyberspace operation even though the action uses a common transport (such as, the LandWarNet). Similarly, a commander utilizing the land domain, conducting the military decisionmaking process, and transmitting plans to subordinates over a network is not a cyberspace operation. Likewise, inform and influence activities, (IIA) delivered via cyberspace, are not inherently cyberspace operations. Lastly, conducting operations in the physical domains which destroy adversary cyberspace assets are not always considered cyberspace operations. While a mutually supporting relationship with cyberspace operations exists, these types of activities are not uniquely cyber in nature.

c. Given the heavy reliance of joint forces on commercial and military computer networks and civilian infrastructure, joint forces must defend key systems and ensure the continuity of critical network functions. Commanders employ an information system that facilitates partner integration, and provides the ability to collaborate across multiple security levels segregated hardware systems.

d. Generating combat power though the operations process.

(1) Cyberspace is a fully operational and contested domain from which future Army forces will gain, maintain, and exploit advantages over adversaries in cyberspace. Commanders apply combat power through the WfFs using leadership and information.[22] Therefore, the Army must generate the cyberspace expertise necessary to support USCYBERCOM, geographic combatant commanders (GCC) and Army commanders at all levels of command. This cyberspace expertise, distributed among several warfighting specialties, is an integral part of the personnel component of the MCS, and essential to the ability to achieve effects in and through cyberspace.[23]

Cyberspace in the motor pool

Army test, measurement, and diagnostic equipment's (TMDE) software is routinely updated through connectivity provided by the Army mission command system. An adversary conducts an offensive cyberspace operation (OCO) to install malicious code on the test equipment. When the test equipment connects to the vehicle, the malicious code disables the computer processor which controls the fuel system, rendering the vehicle inoperative.

The Army must conduct defensive cyberspace operations to ensure the integrity and availability of the equipment, as Army vehicles and TMDE have embedded processors and software.

Preventing this attack should have begun with the acquisition of both the TMDE and the vehicle and continued with the defense of the mission command system during daily operations.

(2) Network, intelligence, and cyberspace experts will build, operate, maintain, and aggressively defend the LandWarNet and, as required, other friendly networks, and attack, deny and exploit adversary networks. Experts will forensically analyze, fight through, and restore capabilities either denied or degraded due to attacks and intrusions. They will conduct active reconnaissance and surveillance to find and track intruders and attackers inside and outside the LandWarNet; and, as necessary, conduct remote or close offensive activities (or determine the decisive points against which to conduct physical offensive operations) to degrade, neutralize, defeat, or destroy cyberspace threats. To achieve the capabilities to generate combat power rapidly, the Army must begin an investment strategy focused on closing known gaps in Army cyberspace capabilities.[24]

(3) Defensive cyberspace operations (DCO), under either Titles 10 or 50 USC, must include the ability to conduct reconnaissance of adversary networks and hunt operations within the LandWarNet (or other friendly networks) to search for threat activity, and identify exploitable vulnerabilities.[25] Army forces, and more specifically, the Army National Guard, will assist federal, state, and local governments with cyberspace capabilities and expertise, when directed or requested, in support of defense support of civil authorities (DSCA) or homeland defense. Similarly, Army forces will also help global partners develop the capability to build, restore, operate, test, and defend their own military networks.[26]

(4) Concurrently, commanders must understand, visualize, describe, direct, lead, and assess the cyber electromagnetic aspect of operations as part of their overall roles in the operations process. Staffs must understand how to integrate cyberspace operations and direct cyber electromagnetic activities (CEMA) to maximize freedom of action in cyberspace and the EMS while denying the same to adversaries. This includes an appreciation of these mediums as maneuver space; that is, areas where positional advantage is possible.

(5) Future Army forces will increase overall situational understanding with the inclusion of cyberspace and the EMS as an essential part of the common operating picture. This added situational understanding includes visibility of friendly, threat, and other specified cyberspace warfighting capabilities, and will depend upon the ability to conduct accurate battle-damage assessments. Future Army forces will be able to see through the cyberspace "noise" and quickly recognize a determined cyberspace attack, identify the quality of attack, and understand the operational impact. Future Army forces will achieve greater understanding of the impacts of offensive and defensive cyberspace activities conducted against threats—including potential second, third, and higher-order effects. The capability to conduct reconnaissance and surveillance to find, fix, and finish cyberspace threats inside and outside the LandWarNet, and forensically analyze an attack or intrusion, will be central to accurate friendly and enemy battle-damage assessments. Robust all-source intelligence support to CEMA is essential and will reduce uncertainty, mitigate risk, and support quality decisions.

e. Cyberspace operations require organizations which are responsive to the needs of operational commanders. Army force structure to support cyberspace operations under Title 10 USC authorities must include organic organizations at operational and tactical echelons, and regionally aligned teams to conduct Titles 10 and 50 USC missions. Cyberspace operations require scalable and tailorable organizations that can increase in capacity and capability based upon the environment.

f. Key to enabling operations is the use of a single lexicon. Use of commonly understood terms and doctrinal missions will enable commanders to visualize and communicate operations, missions, and tasks in the cyberspace domain.

g. Training units and Soldiers to operate in the cyberspace domain requires adaptations to doctrine and training facilities. Individual training must expand beyond information assurance, and transition from passive defense to an aggressive involvement in DCO from all Soldiers and civilians, and family members. At the unit level, the Army must provide the expertise and

capabilities to conduct force-on-force cyberspace engagements to develop unit's abilities to operate in a contested cyberspace domain.

h. Operations in cyberspace present commanders with both challenges and opportunities not encountered in the physical domains. Many challenges are linked to policy and legal restrictions on a commander's ability to conduct operations. The opportunities arise from the very nature of the domain. Because cyberspace is a virtual domain, many of the enablers reside in the physical domains. Commanders may address adversaries in cyberspace, or conduct operations in the physical domains to deny, degrade, or destroy enablers of cyber terrain.[27]

4-2. Conducting operations in cyberspace

a. The network has human, physical, and virtual aspects. Nearly all networks are part of the cyberspace domain but are rooted in the human users resulting in a virtual extension in and through cyberspace to conduct operations. Commanders visualize operationally relevant activity across both physical and virtual domains as continuous and interrelated; conduct simultaneous, linked operations across all domains and the EMS; engage populations wherever they live and operate; and tailor the full range of destructive, constructive, and information capabilities into combinations that address the underlying motivations for group behavior. Adopting this approach provides future formations with the intellectual means to gain unprecedented understanding, range, speed, operational and organizational agility, influence, and achieve mission success.

b. Commanders conduct operations in and through cyberspace to gain and maintain freedom of action while denying the same to adversaries. Operations span steady state operations, all phases of a campaign, and the ROMO. These operations are integrated through the operations process, focus on the AO and area of influence, and support the development of situational understanding in the commander's area of interest.

c. The Army utilizes the LandWarNet, a component of the MCS, to conduct operations. Army signal corps organizations conduct Title 10 missions, and support Title 40 and 44 USC requirements, through the building, operating, and defending the LandWarNet and other specified cyberspace, all influenced by an understanding of adversary capabilities.[28]

d. Army intelligence capabilities operate in both a Title 10 USC and Title 50 USC capacity to enable operations. Intelligence capabilities are critical to selecting and prioritizing cyberspace targets and the appropriate response as part of the targeting process, and developing situational understanding to support the overarching operations process.

e. The OE drives commanders to utilize all domains to conduct unified land operations. Commanders must operate in cyberspace to gain and maintain freedom of action while denying the same to adversaries. Convergence applies to both the technological and psychological aspects of achieving cross-domain synergy. Army leaders readily accept technological convergence, but they do not have the same level of acceptance for psychological convergence, especially the idea of operating simultaneously in the physical and virtual domains to achieve operational goals. This convergence began when the military and the adversary began to use

commercial information systems, and has steadily grown as capabilities have matured. The Army still struggles to address this convergence as an opportunity ripe for exploitation by a willing adversary or innovative commander.

(1) All military operations will have an aspect of cyberspace operations, particularly defense information network operations (DINO) and DCO. The increasing expansion of cyberspace within the physical domains demands the Army no longer decide an activity is a discretely cyberspace operation. The Army is reliant upon an unseen cyberspace infrastructure from the equipment an individual Soldier carries to major weapon systems. Embedded processors and network-enabled connectivity exist in almost all equipment; therefore, the Army must build, operate, maintain, and defend this portion of cyberspace, as it would other aspects of the MCS.

(2) The military should not automatically categorize operations as either inherently cyberspace or not cyberspace. The Army must recognize the cross-domain relationships and ensure each domain is addressed during operations. Commanders at all echelons must integrate cyberspace activities (OCO, DCO, and DINO) with all operations in the physical domains as part of the operations process.

(3) Achieving cross-domain synergy will first require the joint force to achieve inter-domain synergy; that is, the actions and activities of the joint force and key national assets synchronized in time, space, and purpose. The evolution of the air domain serves as a comparable example. The progression of inter-service coordination, to integration, to component commands, and eventually to a single air operations center allowed the joint force to achieve synergy between the land, air, and maritime operations.

4-3. Enabling and retaining freedom of action while denying the same to adversaries

a. The complexity and lethality of the battlefield demands mastery of combined arms—the full array of joint capabilities across all domains. Army forces find, fix, and finish adversary capabilities on land and in cyberspace to exploit opportunities. This requires leaders to near-simultaneously apply all elements of combat power at the critical time and place to ensure the adversary cannot recover. In addition to physical disadvantages, maneuver in multiple domains imposes a psychological impact, increasing individual fear amongst adversaries leading to a breakdown in unit cohesion.

b. To deny adversaries freedom of maneuver, commanders achieve cross-domain synergy in the conduct of unified land operations. Army commanders are accustomed to integrating air, space, and maritime capabilities and activities during land operations. Commanders must also visualize operationally-relevant activity across both physical and virtual domains; conduct simultaneous, linked operations in land and cyberspace; engage populations in both domains; and address the underlying motivations of the adversary. Preventing the enemy from employing simultaneous offensive and defensive capabilities restricts freedom of maneuver, allowing commanders to seize the initiative in multiple domains.

c. To comply with the requirements of Titles 40, 44 and 47 USC, the Army implements a DOTMLPF approach across the lifecycle of cyberspace capabilities. These responsibilities, and the associated policy and tasks, must be transparent to the operational Army, whether conducting daily operations on a joint installation or deployed in an operation. The risk for the Army is a defensive posture which limits options to exploit opportunities.

(1) The Chief Information Officer of the Army has the responsibility to establish policy and standards to protect the network throughout the lifecycle of the MCS. Capability developers, acquisition agencies, ARCYBER, and applicable network operations (NetOps) elements ensure fielded solutions address these requirements. Responsibility for the planning and execution of DCO resides with NetOps elements overseeing the associated tier of the network.[29] The U.S. Army Network Enterprise Technology Command and its subordinate signal organizations are currently responsible for implementing the technical solution.[30]

(2) Army commanders are responsible for ensuring protection and defense of their portion of the network. DCO integrates through the operations process across all domains. Therefore, DCO is planned and executed within the commander's decision cycle and is viewed as an element of the overall operation. Commanders require the ability to conduct reconnaissance on friendly and adversary networks, and to identify weaknesses in defenses and vulnerabilities in adversary networks. Integral to any DCO is effective leader development and individual training, and the rapid application of new capabilities (especially as it concerns software and hardware). In the end, any network defense policy or operation is commander's business, and cannot limit the commander's freedom of maneuver in any domain.

4-4. Creating operationally significant effects within an AOR

a. Many AOR operations in cyberspace are conducted under Title 50 USC. Army contributions to these activities come from the U.S. Army Intelligence and Security Command and ARCYBER, primarily, in support of USCYBERCOM and the National Security Agency. Army commanders encounter myriad policy constraints to ensure the operations are legal. Most cyberspace operations in support of a GCC are coordinated and executed through USCYBERCOM and the regionally aligned services' cyber component commands per a USCYBERCOM operational directive. These Title 50 USC cyberspace capabilities provide commanders new opportunities to conduct operational preparation of the environment in multiple domains, either sequentially or near-simultaneously.

b. Regionally aligned forces support the operational echelons' (Theater Army and corps) mission to defend the LandWarNet. These forces coordinate with ARCYBER to ensure the correct defensive actions are applied to the network. The operational echelon headquarters integrates these actions through the operations process and staff integrating cells (current operations, future operations, and plans) to address the requirements and capabilities of all WfFs. This ensures actions in the cyberspace domain are linked to desired outcomes in the land domain.

c. These same regionally aligned forces offer capabilities to conduct OCO under Title 10 USC authorities. They integrate with ARCYBER for intelligence and if necessary, technical support to conduct the mission. Commanders retain the authority and responsibility to integrate

OCO with operations in the physical domains to achieve the desired endstate. The operations process remains the key enabler for success; therefore, all OCOs integrate through the operations process and deconflict through the joint targeting process.

d. Providing a commander with organic cyber expertise and a local cyberspace capability allows phase 0-I strategic cyberspace capabilities to transition from strategic to operational echelons. Commanders conducting cyberspace operations under Title 10 USC benefit from the operational preparation of the environment conducted under Title 50 USC and capitalize on all operational domains during phases II-V. Operations under the Title 50 USC authorities continue during phases II-V.

4-5. Creating local effects. Think globally, act locally

a. To be successful during unified land operations, commanders integrate and synchronize all actions across all domains through mission command. Commanders supported by their staffs, integrate CEMA as part of their overall combined arms employment of capabilities.[31]

b. Cyberspace capabilities must be responsive and available without lengthy approval cycles. Commanders must trust that cyberspace operations are agile, responsive, and timely. In the future, commanders access cyberspace capabilities to conduct operations under their Title 10 USC authorities to achieve local effects without having to leverage Title 50 USC assets, which may reside outside their authorities. Commanders require the ability to employ cyberspace capabilities to meet intent and accomplish the mission while denying adversaries freedom of maneuver in cyberspace. This capability allows the commander to take action in cyberspace without creating unintentional collateral effects outside the AO and provides the ability to conduct local cyberspace operations rapidly to take advantage of fleeting opportunities and seize and retain the initiative.

c. Tactical commanders employ organic capabilities to defend their portion of the network. These capabilities are a combination of materiel and non-materiel solutions and are executed in accordance with guidance from USCYBERCOM and/or ARCYBER. The command utilizes the operations process to synchronize and integrate DCO into operations and across WfFs. Training and education is key; leaders, Soldiers, and civilians must understand the critical nature of their roles in protecting the network.

d. Army commanders, from Theater Army to battalion, require the capability to plan and execute the full range of cyberspace operations under Title 10 USC. Tactical commanders utilize the operations process to think globally and identify and develop opportunities to create local effects using organic or task organized capabilities

(1) The doctrinal joint targeting process facilitates the deconfliction of OCO with other operations. Tactical operations are conducted using the commander's inherent Title 10 USC authorities. If the commander cannot achieve the desired effects with organic capabilities, the target is nominated to the next echelon.

(2) Current models for requesting OCO follow the air tasking order model, with USCYBERCOM as the highest tasking authority. However, Army commanders require a process which integrates cyberspace operations into their capabilities, similar to how Army attack aviation is controlled or field artillery fires are provided. For field artillery, organic field artillery battalions provide direct support to a brigade combat team's (BCT) organic maneuver battalions. The BCT also has access to reinforcing and general support fires brigades from the division and/or corps. Finally, the joint force, through the corps and division, allocates capabilities to provide integrated reinforcing fire support to the BCT. These capabilities at the tactical level dictate increased leader development in cyberspace operations.

e. Regardless of echelon, commanders require the ability to seize and retain freedom of maneuver in cyberspace while denying the same to adversaries. Achieving this requires a combination of situational awareness, access to offensive and defensive capabilities, and training.

Chapter 5
Conclusion

a. To be successful during unified land operations, commanders synchronize all WfFs through mission command across the operational domains. Through mission command, commanders initiate and integrate all military functions and actions toward a common goal; that is, mission accomplishment. To accomplish this, commanders require an efficient and effective organizational design which enables cross-domain synergy.

b. The generating force bears the burden to provide the operational force with the cyberspace capabilities to ensure commanders can effectively operate in all domains within their current authorities. It also owes the Army the intellectual framework to be cognizant and competent across all domains and the EMS. This will require a reevaluation of responsibilities across the generating force to develop integrated DOTMLPF solutions, including an effective research development, test, and evaluation way-ahead. The generating force must also provide operational commanders with a DOTMLPF solution which transitions the burden from the Soldier to technology, seamlessly operates across the ROMO, and enables effective home station training. These solutions require clearly defined roles and responsibilities amongst joint and Army force modernization proponents, capability developers, research and development organizations, training developers, and the acquisition community.

c. To enable commanders to conduct cyberspace operations effectively and efficiently, the Army must collectively answer the following interdependent questions.

(1) How can the Army fully leverage DOTMLPF activities to integrate the necessary unified action partner teams that effectively and efficiently allow for the achievement of a broad range of capabilities and support Army operations regardless of which authority a commander is under?

(2) How can the Army achieve unity of effort when developing the resources to conduct cyberspace operations as part of unified land operations to achieve effects in and through cyberspace?

(3) What is the best organization to integrate and synchronize concepts and capabilities development for cyberspace capabilities as an element of combined arms to ensure those capabilities are available across the ROMO?

(4) How can the Army enable commanders to take action under Title 10 utilizing cyberspace capabilities within their assigned AO to retain initiative in cyberspace and achieve cross-domain synergy?

(5) What are the operational benefits of creating a cyberspace WfF?

(6) What is the most effective organizational construct to conduct OCO to ensure cyberspace operations are integrated with operations in other domains?

(7) What is the most effective construct to integrate policy, processes, and organizations for DCOs to ensure the requirements of USC are met and DCOs are integrated with operations in other domains?

(8) How can the Army simplify the network architecture and provide intuitive user interfaces and tools to conduct cyberspace operations efficiently at all echelons as part of unified action?

(9) How can the Army develop and maintain its cyberspace expertise to efficiently gain and retain the skills necessary to conduct cyberspace operations without sacrificing effectiveness?

(10) How can the Army educate and train its commanders, leaders, and units to think and act effectively across all domains and the EMS?

(11) How must the institutional force be adapted to ensure the Army can effectively integrate its responsibilities to man, train, and equip Army organizations as it develops its cyberspace capabilities?

(12) How does the Army attract, select, train, and retain cyber warriors?

Appendix A
References

Section I
Annotated Required References. Army regulations, DA pams, field manuals, Army doctrine publications (ADP), doctrine reference publications (ADRP), and DA forms are available at Army Publishing Directorate Home Page http://www.usapa.army.mil TRADOC publications and forms are available at TRADOC Publications at http://www.tradoc.army.mil/tpubs Joint pubs are available on the Joint Electronic Library at http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm or https://jdeis.js.mil/jdeis/index.jsp?pindex=0

Department of Defense Strategy for Operating in Cyberspace(2011, Jul). Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Cyberspace is redefining security. DOD faces cyberspace opportunities and challenges. This document assesses these and sets a strategy for approaching the cyber mission.

Section II
Annotated Related References

Amos, J. (2012, Nov). Who We Are. Proceedings Magazine. Vol. 138/11/1,317. United States Naval Institute. Retrieved from http://www.usni.org/magazines/proceedings/2012-11

The Marine Corps remains a constant in the Nation's defense. Marines play a key role in the warfighting heritage of the nation. The Marine Corps is but one arm of a team. On the modern battlefield, no element of the joint force fights alone.

Applegate, S. (2012, Jun 6). The principle of maneuver in cyber operations. George Mason University. Retrieved from http://ebookbrowse.com/2012-the-principle-of-maneuver-in-cyber-operations-pdf-d443090774

Explores maneuver in cyber operations, looking at concept of maneuver and uses it to define and explore the characteristic of maneuver in cyberspace. Examines both offensive and defensive cyber maneuver and discusses kinetic analogies. Touches on sovereignty in cyberspace as it relates to cyber maneuver.

Booz Allen Hamilton©. (2010). Cyber 2020, Asserting Global Leadership in the Cyber Domain. McLean: VA. Retrieved from http://www.boozallen.com/media/file/cyber-vision-2020.pdf

The U.S. must develop a strategy that focuses on more than technology to retain its status as a cyber power.

Chairman of the Joint Chiefs of Staff (CJCS). The national military strategy for cyberspace operations. (2006, Dec). DC. Retrieved from http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

Describes cyberspace domain, articulates cyberspace threats and vulnerabilities, provides strategic framework for action and strategic approach for using cyberspace operations.

CJCS Instruction 6510.01F. (2011, FEB 9). Information assurance and support to computer network defense. DC. Retrieved from http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
Provides information assurance and support to computer network defense.

CJCS Manual 6510.01B. (2012, Jul 10). Cyber incident handling program. DC. Retrieved from http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
Describes the DOD cyber incident handling program its major processes, implementation requirements, and related U.S. government interactions.

DOD. (2011, Nov). Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011. Section 934. DC. Retrieved from www.defense.gov/news/d20110714cyber.pdf
Report answers thirteen questions posed in Senate Report 111-201.

DOD Strategy for Operating in Cyberspace. (2011, Jul). DC. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf
Defines cyberspace as operational domain, describes strategy to utilize and protect cyberspaces assets.

Department of Defense Directive (DODD) 5144.1. (2005, May 2). Assistant Secretary of Defense for Networks and Information Integration [subject]. DC. Retrieved from http://www.dtic.mil/whs/directives/corres/dir.html
Assigns responsibilities, functions, relationships, and authorities to the assistant Secretary of Defense for networks and information integration/DOD chief information officer (CIO).

DODD 8000.01. (2009, Feb 10). Information Enterprise Management [subject]. DC. Retrieved from http://www.dtic.mil/whs/directives/corres/dir.html
Provides direction on management of the DOD Information Enterprise.

DODD 8500.01E. (2009, Feb). Information Assurance [subject]. DC. Retrieved from http://www.dtic.mil/whs/directives/corres/dir.html
Establishes policy and assigns responsibilities to achieve DOD information assurance.

Joint Operational Access Concept. Version 1.0.
Identifies how joint forces will operate in response to antiaccess and area denial challenges.

Air Force Doctrine Document 3-12
Cyberspace Operations (Change 1)
Establishes fundamentals for Air Force cyberspace operations.

ADP 3-0
Unified Land Operations
Explains that cyber electromagnetic activities are primary staff tasks of mission command.

ADRP 3-0
Unified Land Operations
Describes how the Army fights in sustained land operations through simultaneous offensive, defensive, and stability operations.

ADRP 6-0
Mission Command (Change 1)
Discusses mission command as a foundation for unified land operations.

Army Regulation (Reg) 25-1
Information Management, Army Knowledge Management and Information Technology
Establishes policies and assigns responsibilities for information management and information technology.

Army Reg 25-2
Information Management, Information Assurance, Rapid Action Revision
Provides information assurance policy, mandates, roles, responsibilities, and procedures for implementing the Army information assurance program.

DA Pam 25-1-2
Information Management: Information Technology Contingency Planning.
Provides operational procedures and practical guidance for information technology contingency planning to support Army organizations.

Field Manual (FM) 3-13
Inform and Influence Activities
Provides doctrinal guidance and directions for conducting inform and influence activities and discusses the importance of information in operational environments.

FM 3-36
Electronic Warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

FM 6-01.1
Knowledge Management Operations
Provides doctrinal guidance for organization, operations, principles, tactics, techniques, and procedures necessary for effective knowledge management integration.

FM 6-02.70
Army Electromagnetic Spectrum Operations
Overview of electromagnetic spectrum operations at the strategic, operational, and tactical levels, policy implementation, and host nation coordination.

FM 6-02.71
Network Operations
Doctrinal foundation for network operations.

Hayden, M. (2011, Spring). The future of things cyber. *Strategic Studies Quarterly*: AL: Air University Press. Vol. 5, 3-7. Retrieved from http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf
Former Director of the National Security Agency and the Central Intelligence Agency discusses cyber questions.

Joint Publication (JP) 2-01
Joint and National Intelligence Support to Military Operations
Describes how joint and national intelligence operations support military operations.

JP 3-0
Joint Operations
Foundation and fundamental principles that guide the Armed Forces in joint operations.

JP 3-12
Cyberspace Operations
Joint doctrine for the planning, preparation, and execution of cyberspace operations.

JP 3-13
Information Operations
Joint doctrine for information operations.

JP 3-13.1
Electronic Warfare
Provides joint doctrine for the planning, execution, and assessment of electronic warfare across the range of military operations.

JP 3-14
Space Operations
Joint operational principles associated with support from, through, and operating in space.

JP 3-27
Homeland Defense
Joint doctrine for the defense of the U.S. homeland across the range of military operations.

JP 3-28
Civil Support
Doctrine for planning and conducting joint civil support operations.

JP 3-30
Command and Control for Joint Air Operations
Joint doctrine for the command and control of joint air operations across the ROMO.

JP 3-31
Command and Control for Joint Land Operations
Joint doctrine for command and control by a joint force land component commander.

JP 6-0
Joint Communications Systems
Doctrine for communications system support of joint operations across the ROMO.

JP 6-01
Joint Electromagnetic Spectrum Management Operations
Doctrine for EMS management operations in support of joint operations.

Kastenberg, J. (2009). Changing the paradigm of internet access from government information systems: A solution to the need for the DOD to take time-sensitive action on the NIPRNET. In *The Air Force Law Review, Cyberlaw Edition*. Vol 64. 175-209. Retrieved from http://www.au.af.mil/au/awc/awcgate/law/af_law_review_cyber.pdf
The threat to DOD information systems through cyberspace is real, and a defense in depth is required to meet it. The defense should begin with social behavior, modifying the culture of permissive use, but also include technical solutions.

Libicki, M. (2009). Cyberdeterrence and Cyberwar. CA: RAND Corporation. Retrieved from http://www.rand.org/pubs/monographs/MG200/
Addresses pros and cons of counterattack, the value of deterrence and vigilance, and other actions the U.S. takes to protect itself against deliberate cyber attacks.

Libicki, M (2012). Cyberspace is Not a War-Fighting Domain. In *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8:2. OH. Moritz College of Law. 321-336. Retrieved from http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf
Essay argues the notion that cyberspace is a warfighting domain is misleading and pernicious.

McHugh, J. & Odierno, R. (2012, Feb 17). The Posture of the United States Army. [Statement to the Committee on Armed Services U.S. House of Representatives]. Retrieved from http://www.au.af.mil/au/awc/awcgate/army/armyposture2012.pdf
Summary of Army activities and achievements for FY 2011 with a look towards transition and the future.

Porche, I., Paul, C., York, M., et al. (2012). Redefining information warfare boundaries for an Army in a wireless world. CA. RAND Arroyo Center. Retrieved from http://www.rand.org/pubs/monographs/MG1113.html
Compares the emerging doctrine of cyber operations to clarify prevailing boundaries between the areas of interest and the expected progression of these boundaries in the near future. Offers new definitions for activities such as information warfare.

Schaap, A. (2009). Cyber warfare operations: Development and use under international law. In *The Air Force Law Review, Cyberlaw Edition*, Vol. 64. Retrieved from http://connection.

ebscohost.com/c/articles/45162334/cyber-warfare-operations-development-use-under-international-law
The article presents a discussion of the development and use of cyber warfare operations under international law.

Schilling, J. (2010). Defining our national cyberspace boundaries. PA. Army War College.
Currently the U.S. has no policy that articulates a cyberspace boundary framework. Retrieved from http://www.hsdl.org/?view&did=12135
Paper discusses need to identify national cyberspace boundaries before the U.S. can define and defend hostile acts and intent by cyberspace adversaries.

Todd, Graham H (2009). Armed attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition. In *The Air Force Law Review, Cyberlaw Edition*, Vol 64, 65-102. Retrieved from http://www.au.af.mil/au/awc/awcgate/law/af_law_review_cyber.pdf
There is currently no international, legally binding instrument that addresses cyberspace attacks as threats to national security.

TRADOC G2. (2012, Aug). Operational Environments to 2028: The Strategic Environment for Unified Land Operations.
The Army must strive to understand the future and prepare to operate in any environment.

TRADOC Pam 525-2-1
The United States Army Functional Concept for Intelligence 2016-2028
What the Army must do to develop forces capable of conducting intelligence in the future OE.

TRADOC Pam 525-3-0
The U.S. Army Capstone Concept
Describes what the Army must do in the future to prevent, shape, and win, and the capabilities it will require to accomplish these missions in the future OE.

TRADOC Pam 525-3-1
United States Army Operating Concept
Describes how Army forces conduct operations as part of the joint force to deter conflict, prevail in war, and succeed in a wide range of contingencies in the future OE.

TRADOC Pam 525-3-3
The United States Army Functional Concept for Mission Command 2016-2028
Describes how Army forces apply mission command during operations, and identifies the required capabilities.

TRADOC Pam 525-3-5
The United States Army Functional Concept for Protection 2016-2028
Describes how the future Army force protects personnel and vital assets in the OE.

TRADOC Pam 525-5-600
The United States Army's Concept of Operations LandWarNet 2015

Addresses how LandWarNet enables leader-centric operations in a fully networked and global collaborative context in the future operational environment.

TRADOC Pam 525-7-8
Cyberspace Operations Concept Capability Plan 2016-2028.
Addresses cyberspace capabilities necessary for success in the future operational environment.

USC Title 10§2224 - Defense information assurance program. (2011). Section 2224. Retrieved from http://uscode.house.gov/lawrevisioncounsel.shtml
Statutory authorities for the Secretary of Defense to establish the Defense Information Assurance Program.

USC Title 10§ 2223 – Information technology: Additional responsibilities of the chief information officer. Retrieved from http://uscode.house.gov/lawrevisioncounsel.shtml
Statutory provisions that assign additional responsibilities of the DOD CIO.

USC, Title 40, Subtitle III – Information technology management. Retrieved from http://uscode.house.gov/lawrevisioncounsel.shtml

USC, Title 44§3541-§3549 – Federal Information Security Management Act of 2002. Retrieved from http://uscode.house.gov/lawrevisioncounsel.shtml
Statutory authorities that enhance management and promotion of electronic government services and processes; establishes a federal CIO within the office of management and budget, establishes broad framework of measures that require using Internet-based information technology for citizen access to government information and services, and for other purposes.

USC Title 47, Chapter 9 – Interception of digital and other communications. Retrieved from http://uscode.house.gov/lawrevisioncounsel.shtml

USC Title 50 – War and National Defense. Retrieved from http://uscode.house.gov/download/title_50.shtml

---

Appendix B
Cyberspace framework

a. Recognizing that no single nation, government agency, or DOD service controls cyberspace operations, USCYBERCOM established a framework for the conduct of its cyberspace mission area.[32] The framework consists of the three operations discussed below.

(1) DINO. These are operations to design, build, configure, secure, operate, maintain, and sustain the DOD information network to create and preserve information assurance. These are viewed traditionally as the "provide and operate" part of the traditional network operations, "operate and defend" mission.

(2) DCO. These are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and net-centric capabilities.

(3) OCO. These operations project power against adversaries in or through cyberspace.

b. Regardless of the type of authority under which they are authorized, Army forces operate within this framework. Army cyberspace capabilities are DINO, DCO, and OCO which provide the commander the capability to deliver effects inside and outside friendly networks and provide the necessary situational awareness of cyberspace and the EMS.

c. Joint doctrine and the Army's doctrinal framework for unified land operations recognizes cyberspace as a domain, but not a WfF. WfFs are conducted in all domains, including cyberspace, and just as with other domains, the commander synchronizes all WfFs through mission command in cyberspace. Essentially, cyberspace is pervasive in all operations and is not solely under the purview of a single branch, function, or WfF. Because of this, Army commanders act in and otherwise utilize cyberspace just as they act and utilize the physical domains. Commanders and leaders must be cognizant and competent regarding how they conduct operations in all domains and the EMS.

Appendix C
Risks and opportunities for the Army in cyberspace

a. The U.S. Army identifies cyberspace as an essential aspect of both the operational environment and unified land operations.[33] The proliferation and reliance upon technology makes U.S. Army forces, from Headquarters, DA through the individual Soldier, vulnerable to adversary activities in cyberspace. The application of these technologies offers opportunities to integrate and conduct operations in multiple domains simultaneously to achieve decision. Army leaders must balance the risks with the opportunities to ensure Army forces are capable of seizing and retaining the initiative in all domains.

b. The cyberspace domain and the EMS are important to the conduct of mission command, the other WfFs, and the projection of land combat power. Cyberspace and the EMS grow progressively more congested and contested, while the development of technological capabilities for (and activities conducted within) these realms are becoming more competitive. State and non-state adversaries are constantly probing, monitoring, and attacking U.S. government, military, and industrial networks. As the Nation's (and other partners') reliance on cyberspace increases, (particularly to monitor and control critical infrastructure), so do cyberspace vulnerabilities that adversaries, growing in their capability and technological sophistication, exploit to create devastating and potentially long-term consequences to land operations, the economy, and national security.

c. As technology continues to develop, many cyberspace and EMS capabilities will become interrelated and interdependent.[34] All these capabilities will require integration across the WfFs during unified land operations. Accordingly, the Army must optimize its capability and capacity

to conduct continuous cyberspace operations as a fundamental and inseparable part of unified land operations.

d. As operations against terrorist operatives have shown, the permanency of actions in cyberspace allows the adversary to continue to influence multiple audiences, even after U.S. lethal and nonlethal actions have eliminated the actor. Commanders must respond to this risk through effective cyberspace operations to limit the impact of these information artifacts.

e. Success in the cyberspace domain necessitates a combined arms approach to integrate and synchronize cyberspace operations across multiple WfFs to ensure freedom of action—in cyberspace and on land—while denying the same to adversaries. Conditions in cyberspace will be created by a combination of code-based, electronic, and physical capabilities. Cyberspace capabilities help realize the mission command philosophy and the mission command WfF, and provide a foundation for employing the MCS as a weapon.

g. If the Army is to integrate capabilities in the operating force effectively, it must also adapt how it develops those capabilities. The development of cyberspace and EMS capabilities must have the same unity of effort as that achieved in the delivery of the capabilities to dominate in the land domain. The Army Title 10 USC responsibilities to man, train, and equip the force must be organized to enable operations in all domains in which the Army operates.

h. Ultimately, it will be the knowledgeable, holistic integration of capabilities and a combined arms approach to the employment of cyberspace and EMS capabilities—perhaps in new and innovative ways beyond their originally intended uses—that will enable the MCS to operate to its fullest advantage. This approach allows the Army to maximize the future Army force's ability to manipulate, deny, disrupt, degrade, or destroy threat cyberspace and EMS capabilities during the conduct of unified land operations.

Appendix D
Interaction of CEMA within the operations process

a. Commanders drive the operations process and ensure information related capabilities are integrated. The mission command WfF enables commanders to link cyberspace activities executed under the authorities of Titles 10, 32, and 50 USC, with operations in the physical domains. Commanders use CEMA to gain and maintain advantages in the cyberspace domain and EMS, thereby facilitating overall mission success. Commanders understand that the cyberspace domain and the EMS are part of the AO influence and maneuver space.

b. CEMA are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the EMS, while simultaneously denying and degrading the use of the same to adversary and enemy, and protecting the MCS.[35] CEMA consist of cyberspace operations, electronic warfare, and NetOps. CEMA may employ the same technologies, capabilities, and enablers to accomplish assigned tasks. To succeed in unified land operations, CEMA must integrate and synchronize across all command echelons and WfFs. CEMA can be used to enable IIA and signals intelligence.

c. Throughout the operations process, staffs assist commanders in developing themes and messages to inform domestic audiences and influence foreign friendly, neutral, adversary, and enemy populations. Staffs assist the commander in employing these capabilities to inform and influence target audiences to shape the OE, exploit success, and protect friendly vulnerabilities. All assets and capabilities at a commander's disposal have the capacity to inform and influence to varying degrees. Cyberspace can be used to research and identify cultural and economic understanding of a target population. Commanders must recognize cyberspace is one mechanism to enable information-related capabilities to deliver information.

d. As the Army builds capabilities to shape and influence the JIE, the barriers to staff interdependence begin to erode, allowing commanders to synchronize the cyberspace as they currently synchronize operations in the land, sea, and air.[36] Evolving from integrating independent staff actions to a single interdependent staff action provides options to the commander to merge staff tasks. This approach reduces unintentional consequences while maximizing operationally relevant outcomes.

Appendix E
The role of the WfFs in cyberspace

a. To achieve success, Army commanders integrate the activities of all WfFs. While cyberspace operations are a sub-component of mission command, conducting operations in and through the cyberspace domain requires commanders to evaluate the role of each WfF in achieving their objectives.

b. Mission command. The mission command WfF is the related tasks and systems that develop and integrate those activities enabling a commander to balance the art of command and the science of control to integrate the other WfFs. Commanders, supported by their staff, integrate cyberspace operations, EMS management operations, and electronic warfare. The staff tasks within the WfF (CEMA, IIA, knowledge management, information management), and the operations process allow the commander to synchronize actions in cyberspace with actions in the physical domains. This synchronization is executed through the MCS. As a component of the MCS, the LandWarNet provides an environment in which commanders conduct many aspects of cyberspace operations. The LandWarNet provides tactical and operational commanders the ability within their Title 10 USC authorities to develop situational understanding of friendly cyberspace in the AO, area of influence, and the area of interest. Additional mission command WfF tasks include information protection (information assurance and computer network defense), and the installation, operation, and maintenance of the LandWarNet.

c. Intelligence.

(1) The intelligence warfighting function is the related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations. Cyberspace-enabled intelligence is a complementary intelligence capability providing the ability to collect information and produce unique intelligence. Computers, technology, and networks facilitate all-source intelligence, the

intelligence disciplines, and other complementary intelligence capabilities. The appropriate title authority (primarily Titles 10 and 50 USC) for each specific discipline or capability governs the guiding methods and regulations for the conduct of each intelligence discipline or complementary intelligence capability. A combination of intelligence analysis and the collaboration of information concerning activity in cyberspace and the EMS produces cyberspace-enabled intelligence. This intelligence supports cyber situational understanding.

(2) Unlike cyberspace operations, cyberspace-enabled intelligence is intelligence-centric based on collection within cyberspace and does not include operations and dominance within the EMS. The results of CEMA provide intelligence professionals with a significant amount of information concerning both the physical and virtual domains. This complementary intelligence capability includes the integration of intelligence products into staff processes, such as intelligence preparation of the battlefield and targeting. The use of cyberspace-enabled intelligence facilitates an understanding of the threat's capabilities, intentions, potential actions, vulnerabilities, and impact on the environment.

d. Movement and maneuver. The movement and maneuver WfF is the related tasks and systems that move and employ forces to achieve a position of relative advantage over the enemy and other threats. Direct fire and close combat are inherent in physical maneuver, and there is a parallel idea of maneuver (positional advantage) in cyberspace. This function includes tasks associated with force projection related to gaining a positional advantage over the enemy. Movement and maneuver in cyberspace is linked to movement and maneuver in the physical domains. A key difference when maneuvering in the cyberspace domain is the terrain. When conducting operations in the land domain, the Army must seize terrain, while in cyberspace, the Army can seize other's terrain, but it can also create the terrain. This man-made terrain allows Army forces to maneuver simultaneously in cyberspace and physical domains.

e. Fires. The fires WfF is the related task and systems that provide collective and coordinated use of Army indirect fires, air and missile defense, and joint fires through the targeting process. The fires WfF provides the mechanism to integrate and deconflict offensive cyberspace operations through the joint targeting process.

f. Protection. The protection WfF is the related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission. For cyberspace operations, the protection WfF is primarily focused on the protection of the personnel and physical components MCS.

g. Sustainment. The sustainment WfF is the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance. The sustainment WfF is focused on ensuring the MCS is properly manned and the physical components of the system are available to the commander.

Glossary[37]

Section I
Abbreviations

ADP	Army doctrinal publication
ADRP	Army doctrinal research publication
AO	area of operations
AOR	area of responsibility
ARCIC	Army Capabilities Integration Center
ARCYBER	U.S. Army Cyber Command
BCT	brigade combat team
CEMA	cyber electromagnetic activities
CJCS	Chairman of the Joint Chiefs of Staff
CSA	Chief of Staff
DA	Department of the Army
DCO	defensive cyberspace operation
DINO	defense information network operations
DOD	Department of Defense
DODD	Department of Defense Directive
DOTMLPF	doctrine, organization, training, materiel, leadership and education personnel, facilities
DSCA	defense support of civil authorities
EMS	electromagnetic spectrum
FM	field manual
GCC	geographical combatant command
ICDT	integrated capability development team
IIA	inform and influence activities
JIE	joint information environment
JP	joint publication
MCS	mission command system
NetOps	network operations
OCO	offensive cyberspace operation
OE	operational environment
Pam	pamphlet
Reg	regulation
ROMO	range of military operations
TMDE	test, measurement, and diagnostic equipment
TRADOC	Training and Doctrine Command
U.S.	United States
USC	United States code
USCYBERCOM	U.S. Cyber Command
WfF	warfighting function

Section II
Terms

computer network attack
Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13)

computer network defense
Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks. (JP 6-0)

computer network operations
Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 3-13)

cross-domain synergy
Complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others. (Joint Operational Access Concept)

cyber electromagnetic activities
Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same, and protecting the MCS. (ADRP 3-0)

cyberspace
Global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

cyberspace operations
Employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

defense information network operations (DINO)
Operations to design, build, configure, secure, operate, maintain and sustain DOD network to create and preserve information assurance on the DOD information networks. (JP 3-12)

defensive cyberspace operations (DCO)
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and net-centric capabilities. (Jp 3-12)

domain
Region distinctively marked by some physical feature.

electromagnetic spectrum
Range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. See also electronic warfare. (JP 3-13.1)

electromagnetic spectrum management
Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. (JP 6-01)

electronic warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

inform and influence activities
Integration of designated information-related capabilities to synchronize themes, messages, and actions with operations to inform U.S. and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking. (ADRP 3-0)

information
Meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1)

information assurance
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation, which includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-33)

information environment
Aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information management
Science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products. (ADRP 6-0)

information operations
The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

information protection
Those active or passive measures used to safeguard and defend friendly information and information systems. (ADRP 6-0)

information requirement
Any information element the commander and staff require to successfully conduct operations. (ADRP 6-0)

information system
Equipment that collects, processes, stores, displays, and disseminates information. Includes computers—hardware and software—and communications, as well as policies and procedures for their use. (ADP 6-0)

joint electromagnetic spectrum management operations
Those interrelated functions of frequency management, host nation coordination, and joint spectrum interference resolution that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. (JP 6-01)

knowledge management
The process of enabling knowledge flow to enhance shared understanding, learning, and decisionmaking. (ADRP 6-0)

knowledge transfer
The movement of knowledge—including knowledge based on expertise or skilled judgment—from one person or group to another. (FM 6-01.1)

LandWarNet
The U.S. Army's contribution to the global information grid that consists of the globally interconnected, end-to-end set of U.S. Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand supporting warfighters, policymakers, and support personnel. (Network Enabled Mission Command Initial Capabilities Document)

mission command system
The arrangement of personnel, networks, information systems, processes and procedures, and facilities and equipment that enable commanders to conduct operations. (ADP 6-0)

network operations
Activities conducted to operate and defend the global information grid. (JP 6-0)

offensive cyberspace operations (OCO).
Operations conducted to project power against adversaries in or through cyberspace. (JP 3-12)

warfighting function
A group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and train objectives. (ADRP 3-0)

Section III
Special Terms

computing environment
Minimum standard configuration that will support the Army's ability to produce and deploy high quality **a**pplications quickly while reducing the complexities of configuration, support, and training.

cyber defense
Integrated application of DOD or U.S. Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries to defend designated networks, protect critical missions, and enable U.S. freedom of action.

cyber effect
Outcomes of a cyberspace operation, including the deliberate and unintentional impacts on the operational environment.

cyberspace capabilities
A device, computer program, or technique including any combination of software, firmware, and hardware designed to create an effect in or through cyberspace.

cyberspace capabilities
DCO and OCO facilitated by DINO that provides the capability to deliver effects to a commander.

cyberspace superiority
Degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, sea and space forces at a given time and sphere of operations without prohibitive interference by an adversary

cyberspace support operations
Actions designed to enable offensive, defensive, and DOD information network operations.

cyberspace terrain
Man-made terrain which includes servers, bridges, firewalls, sensors, protocols, operating systems and the hardware that is associated with a computer or processor

electromagnetic spectrum management operations
Interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.

information operations
Integrated employment during military operations, or information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

information-related capabilities
Capabilities, techniques, or activities employing information to effect any of the three dimensions within the information environment to generate an end(s).

joint information environment
Shared information technology infrastructure, enterprise services, and a single security architecture.

knowledge
Information analyzed to provide meaning and value or evaluated as to implications for the operation.

local effect
A change to a condition, behavior, or degree of freedom, or a consequence of an action within cyberspace which does not create an effect outside the AO.

physical domain
Physical feature on the earth – land, air, space, maritime.

virtual domain
Man-made feature residing within the information environment.

Endnotes

[1] Information environment is defined within DOD as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." See JP 3-13 and FM 3-13 for the full doctrinal discussion of the information environment.
[2] The EMS consists of a range of frequencies of radiation including gamma radiation, X-ray radiation, ultraviolet radiation, visible radiation, infrared radiation, terahertz radiation, microwave radiation, and radio waves. The EMS resides in all the physical domains, and is a transport mechanism within the cyberspace domain.
[3] In joint doctrine, information systems consist of "the entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information." U.S. Army doctrine defines information systems as "Equipment that collects, processes, stores, displays, and disseminates information. This includes computers—hardware and software—and communications, as well as policies and procedures for their use."
[4] The commercial and non-commercial systems include domestic and foreign systems. Military systems include DOD, and friendly and adversary military systems.
[5] DOD defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
[6] The internet is a global computer network which "links computer networks all over the world by satellite and telephone, connecting users with service networks such as e-mail and the World Wide Web" – Encarta English Dictionary
[7] The information environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command and control systems, key decisionmakers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information.
[8] DOD defines the joint information environment as "shared information technology infrastructure, enterprise services, and a single security architecture." The JIE is not interchangeable with the information environment.
[9] The JIE is not interchangeable with the information environment. Rather the JIE is one tool commander's have to operate within the information environment
[10] LandWarNet consists of the globally interconnected, end-to-end set of U.S. Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand supporting warfighters, policymakers, and support personnel.
[11] McAfee® Labs 2012 Threats Predictions, retrieved from http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf.
[12] Hacktivism is the use of computers and computer networks as a means of protest to promote political ends.
[13] Cyberspace is defined within DOD as, "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
[14] Strategic Survey 2012: The Annual Review of World Affairs, p. 396
[15] Gen Amos, "Who We Are." Proceedings Magazine - November 2012 Vol. 138/11/1,317.
[16] McChrystal, S., "It Takes a Network", *Foreign Affairs*, March/April 2011.
[17] Virtual personas and partnerships utilizes cyberspace to replicate a unit or Soldier's actions to maintain and mature relations with friendly or neutral populations that was begun with a physical activity such as a training event.
[18] While no DOD or Army definition exists for local effects, this paper defines local effects as "a change to a condition, behavior, or degree of freedom, or a consequence of an action within cyberspace which does not create an effect outside the AO."
[19] The U.S. Army Mission Command CoE has drafted "The U.S. Army Mission Command Strategy, FY 13-19" to facilitate unity of effort as it develops the capabilities to enable the mission command warfighting function.
[20] See the JOAC.
[21] Joint Publication 3-0.
[22] The Army defines combat power as the total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time. (ADPR 3-0)
[23] Digital IIA activities are one of the key nonlethal capabilities reliant on the LandWarNet.
[24] TRADOC's Mission Command ICDT began a cyberspace CBA in MMM 12 and is expected to complete the CBA in MMM13.
[25] Hunt operations are conducted by the joint force to identify and respond to any adversary presence within the JIE. In the land domain, this type of activity is normally associated with the counter-reconnaissance or counter intelligence operations.
[26] TRADOC Pamphlet 525-3-0.
[27] For the purposes of this white paper, cyberspace terrain is defined as man-made terrain which includes servers, bridges, firewalls, sensors, protocols, operating systems and the hardware that is associated with a computer or processor.
[28] LandWarNet moves information through a seamless network that facilitates information-enabled joint warfighting and supporting operations from the operational base to the edge of tactical formations, down to the individual Soldier.
[29] DA General Order 2010-26 assigns responsibility of the "defense of all Army networks" to the Commander, ARCYBER.
[30] The U.S. Army Network Enterprise Technology Command plans, engineers, installs, integrates, protects, defends and operates Army cyberspace, enabling mission command through all phases of unified action partner operations.
[31] ADRP 6-0.
[32] TRADOC PAM 525-7-8, as well as the current cyberspace capabilities-based assessment, lists NetOps, CyberWar, CyberSupport and Cyber SA as elements of cyberspace operations for the Army. These are all mutually supporting elements that allow the Army to gain an advantage, protect the advantage, and place the adversary at a disadvantage. The USCYBERCOM lines of effort are DINO, DCO, OCO and the elements of Army cyberspace operations map over those. Therefore in this proposed Army framework, NetOps = DINO & DCO(-), CyberWar = OCO & DCO(-).(-).
[33] TRADOC Pam 525-3-0
[34] EMS capabilities do not refer exclusively to electronic warfare capabilities; rather, it refers to any weapon or device that makes use of the EMS as part of its functionality.

[35] ADRP 3-0.
[36] The objectives of the joint information environment can be summarized as: defendable and resilient architecture, federated and shared infrastructure, enterprise services, and identity and access management.
[37] This glossary deliberately deviates from Army publication standards. In an attempt to ensure all readers are informed, this glossary includes frequently confused terms, even if those terms do not appear in the body of the white paper.